CYBERSECURITY AND ENGINEERING LAW: LEGAL FRAMEWORK FOR ACCOUNTABILITY AND ETHICAL RISK MANAGEMENT IN SMART INFRASTRUCTURES*

Abstract

The integration of smart infrastructures-ranging from intelligent transportation systems to interconnected energy grids—has amplified both the opportunities and vulnerabilities within contemporary societies. As these infrastructures rely on cyber-physical systems, the stakes of cybersecurity transcend technical contingencies, extending into domains of legal accountability, regulatory compliance, and ethical governance. This paper examines the legal frameworks that underpin accountability in cybersecurity within engineering contexts, situating them against the backdrop of risk society theory and the expanding surveillance economy. It argues that engineering law must evolve to accommodate the dual imperatives of technological innovation and societal protection, thereby ensuring both resilience and public trust. Through an interdisciplinary approach, the analysis explores how regulatory models, professional codes of conduct, and liability regimes intersect with the ethical responsibilities of engineers in designing, maintaining, and governing smart infrastructures. Emphasis is placed on the reflexive role of law-not merely as a mechanism for sanction but as a framework that fosters responsible risk management, anticipatory governance, and ethical accountability in environments where attribution of cyber incidents is often complex and contested. Ultimately, the paper advances a normative claim that effective cybersecurity governance in smart infrastructures requires an integrated legal-ethical architecture that aligns engineering practice with societal values, ensuring both security and legitimacy in an increasingly digitised public sphere.

Keywords: *Accountability, Cybersecurity, Engineering Law, Ethical Risk Management, and Smart Infrastructures*.

1. Introduction

The proliferation of smart infrastructures-spanning Internet of Things (IoT)-enabled power grids, intelligent transportation systems, e-healthcare, and smart cities-has transformed modern societies into highly interconnected environments. These infrastructures, while offering efficiency, resilience, and innovation, are increasingly vulnerable to sophisticated cyber threats. As cyber-physical systems become integral to critical services, the potential consequences of cybersecurity failures escalate from financial loss to systemic disruption, public safety risks, and even national security concerns. Recent attacks on energy pipelines, healthcare databases, and smart grid systems illustrate that vulnerabilities in engineered infrastructures can be exploited with devastating effects.[1] Despite rapid technological progress, the legal and regulatory frameworks governing cybersecurity within engineering contexts remain underdeveloped. Existing laws and policies often struggle to keep pace with the complexity of modern cyber risks and the blurred boundaries of accountability in interconnected infrastructures. The issue is particularly acute where engineering law intersects with cybersecurity: while engineering codes traditionally address safety, reliability, and professional conduct, they seldom anticipate liabilities arising from digital vulnerabilities or algorithmic failures.[2] This gap creates significant ambiguity over who bears responsibility-the engineer, the corporation, or the state-when critical systems are compromised.

The problem therefore lies in the absence of robust, adaptive legal frameworks capable of allocating accountability, enforcing ethical compliance, and integrating cybersecurity standards into engineering law. Without such mechanisms, the risk of regulatory fragmentation increases, leaving infrastructures exposed to systemic cyber threats. Furthermore, ethical principles that should guide responsible cybersecurity practices, such as duty of care, proportionality, and professional responsibility, remain inconsistently embedded within legal structures.[3] This lacuna undermines both public trust and resilience in smart infrastructures. In response, this research sets out three objectives. First, it seeks to analyse the intersections between engineering law and cybersecurity, identifying the extent to which existing doctrines address vulnerabilities in smart infrastructures. Second, it evaluates mechanisms for legal accountability in cyber failures, exploring liability allocation across engineers, corporate entities, and public authorities. Third, it investigates the ethical dimensions of cybersecurity risk management, with a focus on professional responsibility, fairness, and compliance in the design and maintenance of cyber-physical systems. The study is further guided by three research questions. It asks, firstly, what legal responsibilities arise for engineers, corporations, and states when cybersecurity failures occur in smart infrastructures? This question is critical, given the shared yet diffused responsibilities in multi-stakeholder environments. Secondly, it interrogates how engineering law might evolve to address accountability and risk allocation in cybersecurity contexts. This requires consideration of comparative legal frameworks such as the EU's Network and Information Security Directive and the U.S. Cybersecurity Framework, both of which highlight different approaches to risk governance.[4] Finally, it asks which ethical principles should inform cybersecurity compliance in engineering practice, a question that is urgent as professionals

***By Grace Perpetual DAFIEL, PhD, LLM, BL, LLB,** Veritas University Nigeria, Abuja. Email: dafielg@veritas.edu.ng; dafielgrace904@gmail.com, Tel: +2348037008269. ORCID ID 0009-0007-5621-3450

[1] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishers 2014)

[2] Andrew Murray, *Information Technology Law: The Law and Society* (3rd edn, Oxford University Press 2019)

[3] Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017)

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1, 2018) https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf accessed 16 August 2025

navigate the tension between technological innovation and public protection. By addressing these questions, the research contributes to bridging the gap between law, engineering, and cybersecurity. It underscores the necessity for integrated legal-ethical frameworks capable of strengthening accountability, enhancing resilience, and safeguarding public trust in the digital age. Ultimately, the inquiry aims to advance a model where engineering law not only governs technical safety but also provides a normative foundation for cybersecurity in smart infrastructures.

2. Historical Context and Evolution

Engineering law has historically focused on ensuring safety, reliability, and professional accountability in physical infrastructures such as bridges, power plants, and transport systems. Traditional regulatory frameworks emphasised structural integrity, occupational safety, and contractual obligations. However, the digitalisation of engineering practices has transformed the scope of responsibility, introducing new risks that transcend physical harm and extend into the digital domain. The emergence of cyber-physical systems has blurred the boundary between engineering disciplines and information technology.[5] For instance, smart grids rely on embedded sensors and automated control systems, which expose them to cyber intrusions that may cause cascading power outages. While professional codes of conduct (e.g., those promulgated by engineering associations) highlight obligations of competence and public safety, they seldom anticipate liabilities arising from algorithmic decision-making, networked vulnerabilities, or remote cyberattacks.[6] Legal scholarship has noted that this creates a 'normative lag,' where engineering law remains tethered to physical risks while failing to address the hybrid risks introduced by digitalisation.[7] The evolution of engineering law in the digital age therefore requires integration with cybersecurity regulation, recognising that professional responsibility now extends beyond physical safety to encompass resilience against cyber threats. This reorientation challenges both legislators and engineering institutions to redefine standards of care in light of pervasive digital interconnectivity.

3. Conceptual and Theoretical Frameworks

The governance of cybersecurity within smart infrastructures cannot be understood solely through doctrinal law or technical design. Instead, it requires a conceptual framework that integrates socio-legal perspectives, theories of technological risk, and ethical reasoning. This section draws upon socio-legal theory and techno-legal governance, Ulrich Beck's risk society thesis, and selected ethical theories—utilitarianism, deontological ethics, and virtue ethics—to provide an interdisciplinary foundation for examining accountability and risk management in engineering law and cybersecurity.

Law and Technology Interface: Socio-Legal Theory and Techno-Legal Governance

Socio-legal theory emphasises the reciprocal relationship between law and society, recognising that legal norms both shape and are shaped by social practices, technological innovations, and institutional dynamics.[8] In the context of smart infrastructures, socio-legal analysis highlights how legal frameworks must adapt to rapid technological change while simultaneously legitimising governance structures. The interface between law and technology has been explored through the lens of techno-legal governance, which examines how law regulates technological systems and how technology itself functions as a regulatory modality.[9] As Lessig famously argued, 'code is law': technical architectures structure behaviour as effectively as legal rules, meaning that cybersecurity protections embedded in code often regulate conduct without formal legislation.[10] This dynamic complicates questions of accountability in engineering law, since responsibility is diffused between legal institutions, corporate actors, and technical designers. Socio-legal scholarship further suggests that legal frameworks governing cybersecurity in smart infrastructures must be reflexive: they should not only prescribe standards but also evolve in response to technological developments and stakeholder practices.[11] Reflexive law thus provides a valuable lens for understanding how engineering law can embed cybersecurity norms without ossifying into rigid, outdated rules.

Risk Society Theory: Technology-Induced Risks and Legal Implications

Ulrich Beck's risk society thesis offers a critical framework for conceptualising the vulnerabilities inherent in smart infrastructures. Beck argues that late modern societies are increasingly characterised by the production and management of risks that are global, unpredictable, and technologically induced.[12] Unlike traditional risks, which were localised and calculable, modern risks—such as cyberattacks on energy grids or healthcare systems—are diffuse, transboundary, and difficult to allocate. Smart infrastructures epitomise this condition. Cyber vulnerabilities embedded in IoT devices or control systems may be exploited remotely, transcending national borders and undermining traditional models of liability based on territorial jurisdiction.[13] In Beck's terms, these infrastructures embody 'manufactured risks,' where the very technologies designed to deliver efficiency and resilience also generate systemic vulnerabilities.[14] The legal implications of risk society are profound. First, risk allocation becomes contentious, as it is often impossible to attribute a cyber incident to a single

[5] Brownsword, Scotford and Yeung, *Oxford Handbook* (n 3)
[6] Institution of Civil Engineers, *Code of Professional Conduct* (ICE 2017) https://www.ice.org.uk/download-centre/code-of-conduct
[7] Murray, *Information Technology Law (n2*)
[8] Roger Cotterrell, *The Sociology of Law: An Introduction* (Butterworths 1984)
[9] Roger Brownsword, Eloise Scotford and Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017)
[10] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999)
[11] Gunther Teubner, 'Substantive and Reflexive Elements in Modern Law' (1983) 17 *Law and Society Review* 239
[12] Ulrich Beck, *Risk Society: Towards a New Modernity* (Sage 1992)
[13] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001)
[14] Ulrich Beck, *World at Risk* (Polity 2009)

actor, especially where state-sponsored or anonymous attackers are involved.[8] Second, law must grapple with uncertainty: cybersecurity threats cannot always be predicted or quantified, yet legal systems must still allocate responsibility and design preventive frameworks.[9] Beck's framework underscores the necessity for legal systems to move from reactive liability regimes to proactive governance models that integrate risk anticipation, resilience, and precaution into engineering law.

Ethical Theories and Cybersecurity in Engineering Law

Legal accountability in cybersecurity is inseparable from ethical considerations. Ethical theories provide normative foundations for assessing the responsibilities of engineers, corporations, and states in safeguarding smart infrastructures. Three key ethical frameworks-utilitarianism, deontological ethics, and virtue ethics-offer complementary insights.

Utilitarianism emphasises the maximisation of overall welfare by weighing risks and benefits. In the context of smart infrastructures, utilitarian reasoning would support the allocation of resources to cybersecurity measures that yield the greatest reduction in systemic risks and public harm.[15] For instance, investing in resilient energy systems or healthcare cybersecurity may be justified because of the disproportionate social costs of failure. However, critics note that utilitarian calculations may neglect minority rights, particularly where cost-benefit analyses justify surveillance or restrictions that compromise individual privacy.[16]

Deontological ethics, grounded in duty and obligation, stresses the principle that engineers and corporations have a moral duty of care to protect end-users from foreseeable harm, regardless of utilitarian calculations.[17] Embedding strong cybersecurity in infrastructure design transcends efficiency, constituting a legal duty consistent with engineering codes prioritising safety, integrity, and public welfare.[18]

Virtue ethics focuses on the character and integrity of professionals, emphasising prudence, responsibility, and ethical judgment in practice.[19] In cybersecurity, virtue ethics underscores the role of engineers as moral agents who must exercise discretion in balancing innovation with protection. This perspective highlights the cultivation of professional virtues—such as honesty, diligence, and responsibility—as critical to building trust in smart infrastructures.[20] Unlike rule-based approaches, virtue ethics situates cybersecurity within the ethos of professional responsibility, reinforcing the idea that legal compliance alone is insufficient without a culture of ethical practice.

Integrating Legal, Risk, and Ethical Frameworks

Together, these theories provide a comprehensive understanding of cybersecurity governance in engineering law. Socio-legal theory frames cybersecurity as a hybrid construct shaped by norms, institutions, and technological code. Risk society theory underscores the systemic, global, and uncertain nature of cyber threats, necessitating anticipatory and adaptive legal frameworks. Ethical theory offers normative guidance, ensuring reforms emphasise duty, integrity, and public interest. Integrating these perspectives, this research proposes a foundation for advancing accountability, resilience, and ethical risk management in smart infrastructures through engineering law.

4. Methodology

The complexity of cybersecurity in smart infrastructures demands a rigorous and multi-dimensional methodological approach. This research adopts a combination of doctrinal legal analysis, comparative analysis, and case study methodology. Together, these approaches provide both theoretical depth and practical insights into how engineering law can evolve to address accountability and ethical risk management in cybersecurity.

Doctrinal Legal Analysis: Doctrinal research forms the backbone of this study, offering a systematic examination of existing legal principles, statutory provisions, case law, and regulatory instruments relevant to cybersecurity and engineering law. Doctrinal methodology, often described as the 'black letter law' approach, provides clarity on the content, scope, and interpretation of legal rules.[21] It allows for the identification of gaps, inconsistencies, and ambiguities in current frameworks that govern cybersecurity within smart infrastructures. Key sources include national legislation, such as the United Kingdom's Computer Misuse Act 1990, the European Union's Network and Information Security (NIS) Directive 2016/1148, and the United States' Cybersecurity Information Sharing Act 2015. These are analysed alongside international standards, including the ISO/IEC 27001 Information Security Management Systems framework and the NIST Cybersecurity Framework.[22] Case law—though limited in this domain—is also considered, particularly in relation to liability and negligence in technology-related disputes. The doctrinal analysis further extends to professional engineering codes of conduct, such as those promulgated by the Institution of Engineering and Technology (IET), which establish duties of competence, safety, and responsibility.[23] By integrating statutory, regulatory, and professional sources, doctrinal analysis provides a foundation for assessing how legal rules intersect with engineering practice and how they might evolve to embed cybersecurity standards.

---

[15] John Stuart Mill, *Utilitarianism* (Parker, Son, and Bourn 1863)
[16] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019)
[17] Immanuel Kant, *Groundwork of the Metaphysics of Morals* (1785; Allen Wood tr, Yale University Press 2002)
[18] Institution of Engineering and Technology (IET), *Code of Conduct* (5th edn, IET)
[19] Alasdair MacIntyre, *After Virtue* (3rd edn, University of Notre Dame Press 2007)
[20] Michael Davis, *Thinking Like an Engineer: Studies in the Ethics of a Profession* (OUP 1998)
[21] Terry Hutchinson, *Researching and Writing in Law* (4th edn, Thomson Reuters 2018)
[22] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, 2018); ISO/IEC, *ISO/IEC 27001: Information Security Management Systems* (International Organization for Standardization 2013)
[23] IET, *Code of Conduct* (5th edn).

Comparative Legal Analysis: A comparative approach is necessary given the divergent ways in which jurisdictions address cybersecurity regulation and accountability. Comparative law enables the evaluation of different legal systems, identifying both convergences and divergences that may inform best practices.[24] This research focuses on three key models: i) *The European Union (EU):* The NIS Directive imposes binding cybersecurity obligations on operators of essential services. Its successor, the NIS2 Directive (2022), strengthens compliance mechanisms and harmonises security obligations across Member States;[25] ii) *The United States (US):* The NIST Cybersecurity Framework, though voluntary, is widely used and represents a risk-based governance model that encourages flexibility and industry-led compliance;[26] iii) *The African Union (AU):* The Malabo Convention (2014) illustrates regional efforts in cybersecurity and data protection, though its implementation remains limited across member States.[27] The analysis shows regions balancing regulation, standards, and capacity-building, offering insights on harmonising engineering law and evaluating accountability frameworks.

Case Study: Case studies are incorporated to ground the theoretical and legal analysis in practical realities. This method allows for in-depth exploration of how cyber incidents affect smart infrastructures and how accountability has been, or could be, assigned.[28] Three key case studies are examined: i) *Stuxnet (2010)* – The attack on Iranian nuclear facilities demonstrated how cyber tools could cause physical damage to engineered systems, raising questions about liability, state responsibility, and the limits of international law;[29] ii) *Colonial Pipeline (2021)* – A ransomware attack that disrupted fuel supplies in the US, exposing the vulnerability of energy infrastructure and prompting regulatory responses regarding corporate accountability; [30] iii) *Healthcare Cyberattacks during COVID-19 (2020–2021)* – Breaches in hospital systems across Europe illustrated the dual risks of data compromise and operational disruption, highlighting the ethical obligation to safeguard critical public health infrastructures.[31] These case studies illustrate cyber vulnerability consequences, highlight legal application challenges, and generate insights on responsibility allocation and ethical risk management.

Ethical Integration: The research incorporates ethical analysis alongside legal inquiry. Ethical reasoning is applied in evaluating professional duties of care, proportionality in security measures, and corporate responsibilities. This integration reflects a law-in-context approach, recognising that legal accountability cannot be divorced from ethical obligations in the governance of smart infrastructures.[32] For example, in analysing case studies, ethical theories such as deontological duty (engineers' responsibility to prevent harm) and utilitarian risk-benefit reasoning (balancing cost and resilience) are used to complement legal findings. This interdisciplinary orientation strengthens the normative foundation of the research.

Data Sources and Limitations: The study relies on secondary sources: statutes, regulations, case law, professional codes, and academic literature in law, engineering, and ethics. International standards and policy documents from organisations such as ENISA (European Union Agency for Cybersecurity) and the US Department of Homeland Security are also included. Limitations arise from the evolving nature of cybersecurity regulation: legal frameworks are in flux, and empirical case law is sparse. Moreover, jurisdictional fragmentation makes global harmonisation difficult. To address these limitations, the study triangulates doctrinal, comparative, and case study findings, ensuring a balanced and comprehensive analysis. The combination of doctrinal analysis, comparative study, and case-based inquiry provides a robust methodology for examining cybersecurity and engineering law. Doctrinal analysis clarifies the current state of legal frameworks, comparative analysis reveals best practices across jurisdictions, and case studies contextualise theoretical insights. By integrating ethical reasoning, the methodology ensures that legal reforms are evaluated not only for their technical adequacy but also for their normative legitimacy. This methodological pluralism positions the research to contribute both theoretically and practically to debates on accountability, risk management, and ethical compliance in smart infrastructures.

5. Findings

Cybersecurity Beyond Technical Compliance: Findings from the literature review shows significant gaps between technical risk standards and legal or ethical frameworks. For instance, while cybersecurity standards such as ISO/IEC 27001 provide detailed technical guidance, they lack enforceability unless integrated into legal regimes.[33] Also, legal frameworks often lag behind technological change, resulting in reactive rather than proactive governance.[34] Cybersecurity in smart infrastructures extends beyond technical challenges, encompassing legal and ethical dimensions. Current policies inadequately embed ethics, while fragmented jurisdictions permit regulatory arbitrage and diffuse accountability. Scholars

[24] Mark Van Hoecke (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart 2011)
[25] European Union, *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)* [2022] OJ L333/80.
[26] Peter Swire, 'The NIST Cybersecurity Framework: An International Reference' (2019) 36 *Yale Journal on Regulation* 1
[27] African Union, *Convention on Cyber Security and Personal Data Protection* (2014, Malabo Convention)
[28] Robert K Yin, *Case Study Research and Applications: Design and Methods* (6th edn, Sage 2018).
[29] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown 2014)
[30] US Department of Energy, *Colonial Pipeline Cyber Incident Report* (DOE 2021)
[31] European Union Agency for Cybersecurity (ENISA), *Cybersecurity and Hospitals: Increasing Resilience in Healthcare in the Time of COVID-19* (ENISA 2020)
[32] Roger Cotterrell, *The Sociology of Law: An Introduction* (Butterworths 1992)
[33] Dan Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017) doi:10.1093/oso/9780198795674.001.0001.
[34] Luciano Floridi, *The Ethics of Information* (OUP 2013).

advocate integrating technical standards, legal responsibility, and ethical principles-such as duty of care and proportionality-into engineering law. Such harmonisation would address digital vulnerabilities, strengthen systemic resilience, and foster public trust in the governance of increasingly complex infrastructures.

Legal Accountability in Cybersecurity: The findings from doctrinal and comparative analysis reveal that accountability for cybersecurity in smart infrastructures is diffuse, with overlapping duties imposed on engineers, corporations, and states. Professional engineering codes, such as those of the Institution of Engineering and Technology (IET), impose an ethical and professional duty on engineers to prioritise public safety and integrity.[35] This duty, when applied in the context of cybersecurity, extends to ensuring that infrastructures are designed with secure-by-design principles, adequate testing, and continuous monitoring. Case studies such as *Stuxnet* demonstrate the catastrophic consequences when engineered systems lack sufficient security layers, raising questions of whether engineers have adequately anticipated foreseeable vulnerabilities.[36] Corporations also bear a central role, as they frequently own or manage critical infrastructures. Under the EU NIS Directive and its successor NIS2, operators of essential services are explicitly mandated to implement appropriate and proportionate technical and organisational measures to manage cybersecurity risks.[37] In the US, although obligations are less prescriptive, corporate actors adopting the NIST Cybersecurity Framework are expected to implement governance structures that anticipate and mitigate risks. Comparative evidence shows that corporate accountability is more clearly established in mandatory regimes (EU) than in voluntary ones (US), though the latter still incentivises compliance through reputational and financial pressures.

Governments, as regulators and guarantors of national security, are tasked with setting cybersecurity standards and ensuring enforcement. However, the *Colonial Pipeline* incident illustrates how fragmented regulatory regimes can leave critical infrastructures exposed, with government responses often reactive rather than preventive.[38] The research finds that state responsibility also extends into international law, particularly in cases of state-sponsored cyberattacks where attribution and countermeasures remain contested.

Allocation of Liability in Cyber Incidents: Liability allocation in cybersecurity remains highly unsettled across jurisdictions. Doctrinal analysis indicates that traditional tort principles, such as negligence, product liability, and breach of statutory duty, are not always fit for cyber incidents due to the difficulty of proving causation and foreseeability.[39] For example, in cases of ransomware disrupting essential services, it is unclear whether liability should fall on the engineers for design flaws, the corporation for inadequate security investment, or external attackers who may be untraceable. Comparative analysis reveals varied liability approaches: the EU enforces executive accountability, the US relies on contracts and insurance, while Africa and Asia face weak enforcement. Case studies like Stuxnet, Colonial Pipeline, and COVID-19 healthcare breaches illustrate diffuse responsibility, regulatory delays, and limited accountability.

Enforcement Challenges in Cross-Border Cyberattacks: Cross-border enforcement is a persistent challenge in cyber law. Cyberattacks often originate from foreign jurisdictions, involve transnational networks, and affect multinational infrastructures. This undermines traditional legal frameworks rooted in territorial jurisdiction.[40] Beck's risk society theory applies cyber risks are global, attribution-resistant, and accountability-defying. International law remains fragmented, with limited ratification, sovereignty-centred resistance, and reliance on voluntary cooperation, leaving exploitable enforcement gaps.

Risk Management in Smart Infrastructures: The study demonstrates that risk management in smart infrastructures has shifted from a peripheral issue to a central governance priority. As interconnected digital ecosystems grow, infrastructures face cascading failures and systemic cyber threats. Addressing these risks demands more than technical safeguards: it requires embedding cybersecurity into engineering practice, harmonising regulatory frameworks, and fostering multi-stakeholder cooperation. Yet, in practice, corporations rely heavily on contracts and insurance. Both approaches face limits—insurance often excludes state-sponsored attacks under 'act of war' clauses, while contracts struggle with cascading failures. Comparative evidence reveals divergent responses: the US prioritises cyber insurance, the EU regulatory compliance, while African and Asian jurisdictions depend on donor-led capacity building. Ultimately, insurance and contracts may complement regulation, but they cannot replace robust legal accountability frameworks essential for resilience and trust.

Integration of Cybersecurity Standards into Engineering Law: Further, findings indicate that the integration of technical cybersecurity standards into engineering law remains inconsistent. International standards such as ISO/IEC 27001 and the NIST Framework provide detailed guidance for risk management but lack binding force unless adopted into national legal systems. The EU has made progress by embedding technical standards into regulatory obligations through NIS2, requiring operators of essential services to adopt appropriate frameworks. By contrast, jurisdictions with voluntary models' risk

[35] IET, *Code of Conduct* (5th edn.)
[36] Zetter, *Countdown to Zero.*
[37] *Directive (EU) 2016/1148. Ibid*
[38] US Department of Energy, *Colonial Pipeline Cyber Incident Report* (DOE 2021).
[39] Murray, *Information Technology Law: The Law and Society* (OUP 2019)
[40] Susan Brenner, *Cybercrime and Jurisdiction* (Edward Elgar 2012)

underinvestment in security, as seen in the *Colonial Pipeline* case where minimal compliance left vulnerabilities unaddressed.[41]

Engineering law could serve as a bridge by requiring compliance with internationally recognised cybersecurity standards as a condition of professional responsibility. This would ensure that engineers embed resilience into design processes, creating legal as well as technical accountability.

Ethical Compliance Dimensions: Ethical analysis shows engineers must embed cybersecurity in infrastructure design, reflecting duty of care and professional codes. Yet cases like Stuxnet and healthcare breaches expose gaps. Institutionalising cybersecurity in education and accreditation is crucial to counter cost-driven ethical compromises. The integration of cybersecurity into infrastructures often involves extensive surveillance and monitoring, raising ethical questions about proportionality and privacy.[42] Utilitarian ethics may justify widespread monitoring to maximise collective security, yet deontological perspectives caution against infringing fundamental rights.[43] Comparative evidence shows varying balances: EU law, shaped by the General Data Protection Regulation (GDPR), imposes strict limits on surveillance, whereas US models permit broader corporate monitoring under weaker data protection regimes.[44] The research finds that resilience measures must balance effectiveness with legitimacy. Excessive surveillance risks undermining public trust, which is essential for the long-term resilience of infrastructures.

Corporate Governance and the 'Duty of Care' in Protecting Citizens: Corporate governance is increasingly central to ethical compliance. Boards of directors are now expected to treat cybersecurity as a strategic issue, with NIS2 explicitly requiring management accountability for compliance. Ethical theories reinforce this: utilitarianism emphasises collective welfare, deontology insists on corporate duties of care, and virtue ethics underscores integrity and responsibility.[45] Case studies reveal uneven compliance: Colonial Pipeline's delayed disclosures eroded trust, while healthcare breaches highlighted systemic ethical failures. Doctrinal, comparative, and case analyses identify fragmented accountability, uneven risk management, and indispensable ethical compliance. Collectively, findings affirm the need for an integrated legal-ethical framework to strengthen accountability, resilience, and public trust in smart infrastructures.

6. Conclusion and Recommendations

This research explored how engineering law, cybersecurity, and ethical governance intersect in smart infrastructures. As critical sectors digitalise, interconnected systems deliver efficiency but introduce systemic, transnational risks. The study examined how legal frameworks, ethical principles, and professional duties collectively shape accountability and risk management in addressing these cybersecurity vulnerabilities. The study's key contribution is its integration of doctrinal legal analysis, comparative perspectives, and case study insights into a unified framework connecting law, engineering, and ethics. Doctrinal analysis revealed fragmented laws and the absence of explicit cybersecurity duties in engineering codes. Comparative examination of the EU's NIS2 Directive, the U.S. Cybersecurity Framework, and emerging regimes in Africa and Asia highlighted divergent accountability models. Case studies in energy and healthcare exposed weaknesses in liability structures, where accountability is diffuse, remedies are limited, and victims often lack redress. Ethically, the study applied utilitarian, deontological, and virtue ethics to cybersecurity governance, showing that engineers and corporations owe a duty of care beyond compliance, encompassing fairness, proportionality, and integrity. This produced a normative framework for embedding ethics within legal and technical standards, bridging the gap between cybersecurity measures and public trust. Policy implications included harmonised international frameworks, reforms embedding cybersecurity into engineering law, and multi-stakeholder governance distributing responsibility. Collectively, these recommendations strengthen accountability and resilience, contributing to both scholarly debate and policy development in the digital age.

Nevertheless, the study is not without limitations. First, while the doctrinal and comparative analysis provided a strong theoretical grounding, it relied primarily on existing legislation, policy frameworks, and selected case studies. Empirical research-such as interviews with engineers, regulators, or corporate actors-could enrich the findings by offering insights into how legal and ethical principles are applied in practice. Second, the study's comparative scope was necessarily selective: while it focused on the EU, U.S., and illustrative African and Asian regimes, further exploration of other regions, including Latin America and the Middle East, could yield a more comprehensive understanding of global diversity in cybersecurity regulation. Third, the ethical analysis, while rigorous, was primarily conceptual and could benefit from integration with behavioural studies on how engineers and corporations perceive and act on their cybersecurity responsibilities. These limitations also suggest fruitful avenues for future research. One direction is the empirical testing of accountability frameworks in real-world engineering projects, assessing how legal and ethical obligations influence design and decision-making processes. Also, comparative interdisciplinary research examining how cultural, political, and economic factors shape the governance of cybersecurity across different jurisdictions. Additionally, future scholarship could explore the role of emerging technologies—such as artificial intelligence, quantum computing, and blockchain—in transforming both the risks and regulatory challenges of cybersecurity in smart infrastructures. Finally, there is scope for

[41] DOE, *Colonial Pipeline Report* (n 5)
[42] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).
[43] Paul Cornish, 'Cybersecurity and Proportionality in International Law' (2019) 42 *International and Comparative Law Quarterly* 34
[44] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019)
[45] Michael Davis, *Thinking Like an Engineer: Studies in the Ethics of a Profession* (OUP 2018)

developing metrics and methodologies to evaluate ethical compliance in cybersecurity, bridging the gap between normative theory and practical enforcement.

In conclusion, this article demonstrates that cybersecurity governance in smart infrastructures extends beyond technical fixes or national legislation, requiring an integrated framework that harmonises law, embeds ethical responsibility, and fosters multi-stakeholder collaboration. Combining doctrinal, comparative, and ethical analysis, the study advances scholarship in engineering law and cybersecurity while outlining concrete reform pathways. In an era of technological interdependence and systemic risks, such integration is essential—not simply as regulatory design, but as a vital safeguard for the infrastructures underpinning modern societies and sustaining public trust in the digital age.

This study highlights fragmented legal and ethical frameworks in cybersecurity for smart infrastructures. With rising vulnerabilities in healthcare, energy, and transport, policy must advance toward harmonised, ethically grounded governance. Key implications include international harmonisation, reforming engineering law, and fostering multi-stakeholder models to ensure accountability, resilience, and trust.

Need for Harmonised International Legal Frameworks: One of the most pressing challenges revealed by the research is the lack of harmonisation across jurisdictions. Cyberattacks are inherently transnational: they exploit global digital networks, traverse borders instantaneously, and often involve actors situated in multiple states. Existing instruments, such as the Budapest Convention on Cybercrime, have provided a foundation for cross-border cooperation, but limited ratification and divergent national security priorities reduce its effectiveness.[46] Policy reform must therefore prioritise the creation of a more inclusive and universally ratified legal framework. Such a framework should establish common definitions of cyber incidents, minimum security standards, and uniform rules for cross-border investigation and evidence-sharing.[47] The NIS2 Directive offers a model of binding obligations within a regional bloc; however, without global alignment, attackers can exploit regulatory arbitrage by operating from jurisdictions with weak or absent regimes.[48] An international treaty or framework, potentially under the auspices of the United Nations, should integrate cybersecurity into critical infrastructure protection norms, emphasising both state obligations and corporate duties. Moreover, it should clarify principles of state responsibility in cases of state-sponsored cyberattacks, addressing attribution challenges and outlining proportionate countermeasures in line with international law.[49] Without such harmonisation, accountability will remain elusive, and smart infrastructures will remain vulnerable to systemic failures.

Engineering Law Reform to Incorporate Cybersecurity Standards: Engineering law must recognise cybersecurity as central to public safety rather than a technical add-on. Professional codes emphasise diligence and integrity but rarely specify cybersecurity duties. Reform is needed across regulation, accreditation, and liability. Statutes should mandate compliance with international standards, while revised education and accreditation must institutionalise cybersecurity training, embedding resilience into engineering practice.[50] Also, Liability regimes must reflect shared responsibility between engineers and corporations. Assigning accountability for foreseeable flaws, as in NIS2, deters cost-cutting, drives compliance, and reinforces the ethical duty of care.

Promotion of Multi-Stakeholder Governance Model: Cybersecurity in smart infrastructures cannot be effectively managed by any single actor. The complexity of risks and the diversity of stakeholders-governments, corporations, engineers, insurers, and end-users-demand a collaborative governance model. Findings demonstrate that siloed approaches, whether state-centric or market-driven, consistently fail to anticipate or mitigate large-scale incidents.[51] A multi-stakeholder governance model should operate on three principles: inclusivity, transparency, and accountability based on the following roles:

Role of the State: Within a multi-stakeholder governance framework, the State holds a foundational responsibility to establish clear and robust legal and regulatory standards that provide a secure baseline for IoT development and deployment. Upholding the principle of inclusivity, governments must ensure that regulations are formulated through consultative processes that consider the interests of diverse stakeholders, including industry actors, civil society, and end-users with gender bias.[52] Through transparency, governments should enact accessible and comprehensible rules, accompanied by open enforcement mechanisms that foster public trust. Equally critical is accountability, which requires states not only to ensure compliance through effective oversight but also to safeguard fundamental rights. This entails balancing national security and public safety imperatives with the protection of privacy, data integrity, and individual freedoms, particularly in contexts involving surveillance.[53] Furthermore, governments must promote international cooperation to harmonize standards, reduce regulatory fragmentation, and address the cross-border nature of IoT ecosystems.

[46] *Convention on Cybercrime (Budapest Convention)* ETS 185 (2001).
[47] Susan Brenner, *Cybercrime and Jurisdiction* (Edward Elgar 2012)
[48] *Directive (EU) 2022/2555 (NIS2 Directive)* [2022] OJ L333/80
[49] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)
[50] Michael Davis, *Thinking Like an Engineer: Studies in the Ethics of a Profession* (OUP 2018)
[51] Ulrich Beck, *Risk Society: Towards a New Modernity* (Sage 1992)
[52] Grace Perpetual Dafiel, 'Legal Analysis of Gender Disparities in Engineering: Perspectives from Engineering Law and Reform Pathways' (2025) 9(8) *International Journal of Research and Innovation in Social Science (IJRISS)* ORCID ID: 0009-0007-5621-3450.
[53] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015)

Role of Corporations and Industry: Corporations, as custodians of smart infrastructures and leaders in IoT innovation, must integrate cybersecurity into governance. Inclusive collaboration—spanning developers to service providers—should shape standards reflecting regulatory, consumer, and societal needs. Commitment to accessible, interoperable design, coupled with transparent disclosure obligations like the EU model, enhances oversight, accountability, and user empowerment in security and data practices.[54] In terms of accountability, corporate boards should bear legal responsibility for cybersecurity governance, including resource allocation, compliance assurance, and liability for negligence. Regular audits, third-party assessments, and demonstrable adherence to technical and ethical standards are indispensable. Through these measures, industry enhances resilience, fosters user trust, and ensures IoT ecosystems align with human rights and the rule of law.

Role of Engineers: Engineers, as architects of IoT systems, play a central role in governance. They must embed accessibility, usability, and equity into infrastructure design, ensuring inclusivity for diverse users. Transparency requires explaining design choices, disclosing limitations, and communicating risks clearly. Anchored in accountability, engineers bear a duty to anticipate cyber threats through robust security- and privacy-by-design principles.[55] Professional associations, working in concert with regulators, should establish sector-specific standards that integrate ethical mandates with technical protocols, ensuring consistent compliance across industries. By aligning professional practice with legal and societal expectations, engineers not only protect infrastructures but also advance an IoT ecosystem that is resilient, rights-respecting, and socially responsive.

Role of Civil Society and End-Users: Civil society, academia, and advocacy groups are vital in aligning IoT governance with the public interest. They amplify marginalized voices, scrutinise corporate and state practices, and demand ethical, lawful accountability. End-users, especially in healthcare, strengthen resilience through secure practices and vulnerability reporting. Institutionalising these roles requires multi-stakeholder councils beyond the Internet Governance Forum, alongside harmonised international legal frameworks embedded in engineering law, to foster resilience, mitigate systemic risks, and secure trust in critical infrastructures.

[54] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019)

[55] Grace Perpetual Dafiel, Chukwudi Victor Odoeme and Dennis Amobi Ugwuja, 'Building Accountability: Legal and Ethical Compliance in Engineering Practice with a Focus on Nigeria' (2025) 1(1) *Veritas University Law Journal*.